

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»



Затверджено рішенням вченої ради ДонНТУ
 Протокол від 24.02. 20 25 р. № 2
 Голова вченої ради _____

/Ольга ПОПОВА/

Освітня програма вводиться в дію з 2024/2025 н.р.
 наказом від 23.02. 2025 р. № 61

(з змінами, внесеними відповідно до рішення
 вченої Ради ДонНТУ від 27.02.2025 р., протокол
 №2, введено в дію наказом від 27.02.2025 р. № 61)

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Кібербезпека»

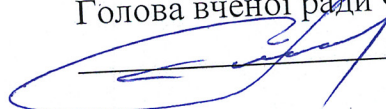
Рівень вищої освіти	Перший	
Ступінь вищої освіти	Бакалавр	
Спеціальність	125	Кібербезпека та захист інформації
Галузь знань	12	Інформаційні технології
Кваліфікація	Бакалавр з кібербезпеки та захисту інформації	

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Освітня програма обговорена та схвалена на засіданні вченої ради факультету комп'ютерно-інформаційних технологій та автоматизації

Протокол № 8 від 20 листопада 2024 р.

Голова вченої ради ФКІТА

 Едуард ПЕТЕЛІН

Освітня програма обговорена та схвалена на засіданні науково-методичної комісії ДонНТУ з галузі знань 12 Інформаційні технології.

Протокол № 5 від 18.11. 2024 р.

Голова НМК 12

 Євген БАШКОВ

Начальник навчально-методичного відділу

« 20 » листопада 2024 р.



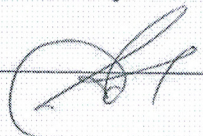
/Ганна ПАНЧЕНКО/

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Освітня програма обговорена та схвалена на засіданні вченої ради факультету комп'ютерних наук і технологій

Протокол № 4 від 24.04. 2020р.

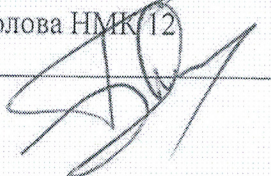
Голова вченої ради ФКНТ

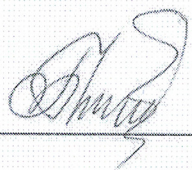
 С.О. Ковальов

Освітня програма обговорена та схвалена на засіданні науково-методичної комісії ДонНТУ з галузі знань 12 Інформаційні технології.

Протокол № 4 від 28.04. 2020р.

Голова НМК 12

 С.О. Башков

Начальник навчально-методичного відділу  /Г. С. Панченко/
« 28 » 04, 2020р.

ПЕРЕДМОВА

Освітньо-професійна програма (ОП) розроблена відповідно до Стандарту вищої освіти за спеціальністю 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти, наказ МОН № 1074 від 04.10.2018 р., з урахуванням змін у Стандарті вищої освіти зі спеціальності 125 Кібербезпека (наказ Міністерства освіти і науки України від 29.10.2024 р. №1547).

Розроблено робочою проектною групою у складі:

Прізвище, ім'я, по батькові		Посада та назва підрозділу (в дужках - за основним місцем роботи)
Керівник робочої проектної групи (гарант освітньої програми):	1. Дорогий Ярослав Юрійович	Професор кафедри прикладної математики та інформатики
Члени робочої проектної групи:	2. Башков Євген Олександрович	Професор кафедри прикладної математики та інформатики
	3. Маслова Наталія Олександрівна	Зав.кафедри прикладної математики та інформатики

Рецензії-відгуки зовнішніх стейкхолдерів (за наявності):

Прізвище, ім'я, по батькові	Посада та назва організації (за основним місцем роботи)
Денис ЗУБКОВ	Заступник директора Департаменту – начальник 5 відділу Департаменту кіберзахисту Адміністрації Держспецзв'язку
Василь ЦУРКАН	доцент Спеціальної кафедри № 5 ІСЗЗІ КПІ ім. Ігоря Сікорського

Освітня програма введена у 2024 р.

Термін перегляду освітньої програми: не менше, ніж раз на 4 роки.

<u>АКТУАЛІЗОВАНО:</u>			
Дата перегляду освітньої програми	21.05.2020	27.01.2022	18.11.2024
Підпис		Зміна назви спец.	Відповідно до внесення змін в стандарт
Прізвище, ім'я, по батькові гаранта освітньої програми	Маслова Н.О.	Назарова І.А.	Дорогий Я.Ю.

Ця освітня програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу ДВНЗ ДонНТУ.

1. Профіль освітньої програми

1.1 – Загальні відомості	
<u>Повна назва вищого навчального закладу (відокремленого структурного підрозділу)</u>	Державний вищий навчальний заклад «Донецький національний технічний університет»
<u>Ступінь вищої освіти та назва кваліфікації мовою оригіналу</u>	Перший (бакалаврський) рівень Бакалавр з кібербезпеки та захисту інформації
<u>Офіційна назва освітньої програми</u>	Кібербезпека
<u>Тип диплому та обсяг освітньої програми</u>	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
<u>Наявність акредитації</u>	Сертифікат про акредитацію серія УД № 05008640, виданий 23.04.2019р. Термін дії сертифіката до 01 липня 2025 р.
<u>Цикл/рівень</u>	НРК України – 7 рівень, FQ-EHEA - перший цикл, EQF-LLL - 6 рівень
<u>Передумови</u>	Умови вступу визначаються «Правилами прийому до ДВНЗ «Донецький національний технічний університет», затвердженими Вченою радою університету. На базі атестата про повну загальну середню освіту
<u>Мова(и) викладання</u>	Українська
<u>Термін дії освітньої програми</u>	до 01.07.2025 р.
<u>Інтернет-адреса постійного розміщення опису освітньої програми</u>	http://wiki.donntu.edu.ua/view/Категорія:Освітні_програми
1.2 – Мета освітньої програми	
Підготовка висококваліфікованих фахівців в галузі інформаційних технологій зі спеціальності 125 Кібербезпека та захист інформації, здатних вирішувати типові та складні завдання та проблеми забезпечення захисту інформаційних ресурсів у кіберпросторі для подальшої професійної діяльності у галузі інформаційної та/або кібербезпеки.	
1.3 – Характеристика освітньої програми	
<u>Предметна область</u>	Галузь знань: 12 «Інформаційні технології» Спеціальність: 125 «Кібербезпека та захист інформації»
<u>Орієнтація освітньої програми</u>	Освітньо-професійна програма пропонує комплексний підхід до вирішення сучасних проблем управління кібербезпекою. Дисципліни та модулі програми засновані на теоретичних знаннях, які тісно пов'язані з практичними навичками. Студенти отримають необхідні навички та знання у забезпеченні захисту об'єктів інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й інформаційні технології.
<u>Основний фокус освітньої програми та спеціалізації</u>	Акцент у освітній програмі робиться на здобутті навичок та знань в галузі захисту інформаційних активів та ґрунтується на здатності випускників здійснювати професійну діяльність на підприємствах, діяльність яких пов'язана з процесами збору, обробки та розповсюдження інформації різного рівня з застосуванням

	інформаційних та комунікаційних технологій.
<u>Особливості програми</u>	Програма зорієнтована на підготовку фахівців, діяльність яких пов'язана з забезпеченням безпеки інформаційних та комунікаційних технологій. Високий рівень дослідницької частини підготовки забезпечується потужною науково-практичною школою на чолі з доктором технічних наук, професором Дорогим Я.Ю., розвинутою міжнародною співпрацею в науковій і освітній сферах
1.4 – Придатність випускників до працевлаштування та подальшого навчання	
<u>Придатність до працевлаштування</u>	Фахівець може займати первинні посади (за ДК 003:2010): Відповідно до здобутого освітнього ступеню бакалавр здатний виконувати професійні роботи за професіями, зазначеними у ДК 003:2010 Національний класифікатор України. Класифікатор професій, а саме: 2139.2. Адміністратор безпеки мереж і систем 2139.2. Фахівець сфери захисту інформації 2139.2. Фахівець з питань безпеки (інформаційно-комунікаційні технології) 2139.2. Конструктор систем кібербезпеки 2139.2. Фахівець з підтримки інфраструктури кіберзахисту 2139.2. Фахівець з реагування на інциденти кібербезпеки 2139.2. Фахівець з криптографічного захисту інформації 2139.2. Фахівець з технічного захисту інформації 2139.2. Фахівець з тестування систем захисту інформації 2139.2. Аудитор інформаційних технологій (з кібербезпеки) 2139.2. Фахівець з оцінки заходів захисту інформації (кібербезпеки)
<u>Подальше навчання</u>	Можливість продовження освіти за другим (освітньо-науковим) рівнем вищої освіти.
1.5 – Викладання та оцінювання	
<u>Викладання та навчання</u>	Студенто-центроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, інформаційна технологія, технологія розвивального навчання, кредитно-трансферна система організації навчання, електронне навчання в системах дистанційної освіти (Moodle), самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами, підготовка кваліфікаційної роботи бакалавра.
<u>Оцінювання</u>	Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою, національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «незараховано») системами. Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Форми контролю: усне та письмове опитування, тестові завдання в тому числі комп'ютерне тестування, лабораторні звіти, презентації, захист курсових робіт та проектів, звітів з практик, захист кваліфікаційної роботи бакалавра.

1.6 Перелік компетентностей випускника

<u>Інтегральна компетентність</u>	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.
<u>Загальні компетентності (ЗК)</u>	<p>ЗК01. Здатність застосовувати знання у практичних ситуаціях.</p> <p>ЗК02. Знання та розуміння предметної області і розуміння професійної діяльності.</p> <p>ЗК03. Здатність спілкуватися державною мовою як усно, так і письмово.</p> <p>ЗК04. Здатність спілкуватися іноземною мовою.</p> <p>ЗК05. Здатність вчитися і оволодівати сучасними знаннями.</p> <p>ЗК06. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>ЗК07. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.</p> <p>ЗК08. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.</p>
<u>Спеціальні (Фахові, предметні) компетенції</u>	<p>ФК01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та Міжнародні вимоги, практики і стандарти у професійній діяльності.</p> <p>ФК02. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.</p> <p>ФК03. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.</p> <p>ФК04. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.</p> <p>ФК05. Здатність відновлювати функціонування інформаційних, інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p> <p>ФК06. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)</p> <p>ФК07. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.</p> <p>ФК08. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.</p>

	<p>ФК09. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>ФК10. Здатність виконувати моніторинг інформаційних, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.</p>
<p>1.7 Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання</p>	
ПРН01.	Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
ПРН02.	Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
ПРН03.	Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
ПРН04.	Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
ПРН05.	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
ПРН06.	Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
ПРН07.	Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
ПРН08.	Застосовувати знання і розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
ПРН09.	Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
ПРН10.	Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
ПРН11.	Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
ПРН12.	Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
ПРН13.	Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.
ПРН14.	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.
ПРН15.	Збирати, обробляти зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводили аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
ПРН16.	Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
ПРН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
ПРН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічною захисту інформації.
ПРН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дії з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

1.8 — Ресурсне забезпечення реалізації програми

<u>Кадрове забезпечення</u>	Викладання професійно-орієнтованих дисциплін здійснюють науково-педагогічні працівники, які мають наукові ступені та вчені звання. До викладання будуть залучені також фахівці, у яких є науковий ступінь та працюють в галузі інформаційних технологій.
<u>Матеріально-технічне забезпечення</u>	Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребі. Користування Інтернет-мережею безлімітне. Для проведення досліджень наявна комп'ютерна техніка.
<u>Інформаційне та навчально-методичне забезпечення</u>	Підручники, навчальні посібники та періодичні наукові видання з інформаційних технологій, захисту інформації та кібербезпеки. Підручники та навчальні посібники до викладання дисциплін циклу професійної підготовки, які розміщені у фонді наукових бібліотек ДВНЗ «ДонНТУ» м. Покровськ, а також Національній бібліотеці України ім. В.І. Вернадського, Інтернет ресурсах та авторських розробках науково-педагогічних працівників ДВНЗ «ДонНТУ». Офіційний веб-сайт https://donntu.edu.ua . містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення освітньо-наукової програми викладені на освітньому порталі: http://donntu.edu.ua .

1.9 - Академічна мобільність

<u>Національна кредитна мобільність</u>	Індивідуальна академічна мобільність реалізується у рамках між університетських договорів про встановлення науково-освітніх відносин для задоволення потреб розвитку освіти і науки з ВНЗ України. Можливість здійснювати підготовку фахівців за індивідуальними програмами, що відповідають потребам конкретного виробництва, згідно з умовами відповідних договорів між університетом і підприємствами.
<u>Міжнародна кредитна мобільність</u>	Не здійснюється
<u>Навчання іноземних здобувачів вищої освіти</u>	Не здійснюється

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

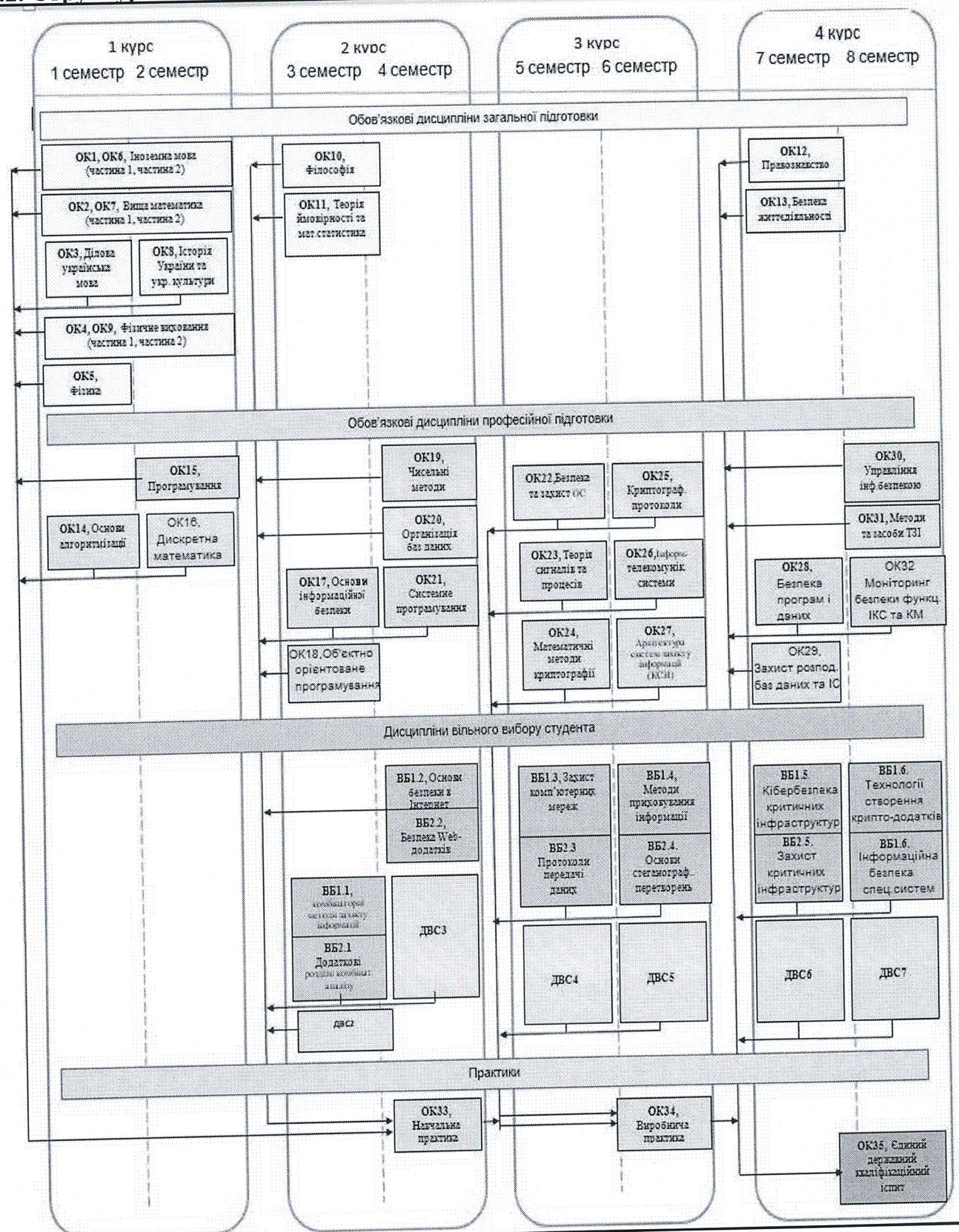
2.1. Перелік компонент ОП

<u>Код компо нента</u>	<u>Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики і атестації)</u>	<u>Кількість кредитів</u>	<u>Форма підсумкового контролю</u>
OK1	Іноземна мова. Частина 1	4,0	екзамен
OK2	Вища математика. Частина 1	7,0	екзамен /ІНД
OK3	Ділова українська мова	4,0	екзамен
OK4	Фізичне виховання (загальна підготовка). Частина 1	3,0	залік
OK5	Фізика	7,0	екзамен
OK6	Іноземна мова. Частина 2	4,0	екзамен
OK7	Вища математика. Частина 2	7,0	екзамен /ІНД
OK8	Історія України та української культури	5,0	екзамен
OK9	Фізичне виховання (загальна підготовка). Частина 2	3,0	залік
OK10	Філософія	4,0	екзамен
OK11	Теорія ймовірностей та математична статистика	6,0	екзамен
OK12	Правознавство	5,0	екзамен
OK13	Безпека життєдіяльності та охорона праці	4,0	диф.залік/ІНД
Всього по циклу:		63	
OK14	Основи алгоритмізації	5,0	екзамен /ІНД
OK15	Програмування	6,0	екзамен /ІНД
OK16	Дискретна математика	5,0	
OK17	Основи інформаційної безпеки	5,0	екзамен /КП
OK18	Об'єктно-орієнтоване програмування	5,0	екзамен /ІНД
OK19	Чисельні методи	6,0	екзамен /ІНД
OK20	Організація баз даних	5,0	екзамен КП
OK21	Системне програмування	5,0	екзамен
OK22	Безпека та захист операційних систем	6,0	екзамен
OK23	Теорія сигналів та процесів	6,0	екзамен /ІНД
OK24	Математичні методи криптографії	6,0	екзамен /ІНД
OK25	Криптографічні протоколи	6,0	екзамен /КП
OK26	Інформаційно-комунікаційні системи	5,0	екзамен /ІНД
OK27	Архітектура систем захисту інформації (КСЗІ)	5,0	екзамен
OK28	Безпека програм та даних	5,0	екзамен /ІНД
OK29	Захист розподілених баз даних та інформаційних систем	6,0	екзамен
OK30	Управління інформаційною безпекою	6,0	екзамен
OK31	Методи та засоби технічного захисту інформації	6,0	екзамен
OK32	Моніторинг безпеки функціонування ІКС та комп'ютерних мереж	6,0	екзамен
Всього по циклу:		105	
OK33	Навчальна практика	4	диф. залік
OK34	Виробнича практика	4	диф. залік
OK35	Єдиний державний кваліфікаційний іспит	1	атестація
Всього по циклу:		9	
Загальний обсяг обов'язкових компонент:		177	
ВБ 1.1	Комбінаторні методи захисту інформації	5,0	диф.залік/ІНД
ВБ 1.2	Основи безпеки в Інтернет	5,0	
ВБ 1.3	Захист комп'ютерних мереж	6,0	екзамен

ВБ 1.4	Методи приховування інформації	5,0	екзамен
ВБ 1.5	Кібербезпека критичних інфраструктур	5,0	екзамен /ІНД
ВБ 1.6	Технології створення криптографічних додатків	6,0	екзамен
ВБ 2.1	Додаткові розділи комбінаторного аналізу	5,0	диф.залік/ІНД
ВБ 2.2	Безпека Web-додатків	5,0	екзамен
ВБ 2.3	Протоколи передачі даних	6,0	екзамен
ВБ 2.4	Основи стеганографічних перетворень	5,0	екзамен
ВБ 2.5	Захист критичних інфраструктур	5,0	екзамен /ІНД
ВБ 2.6	Інформаційна безпека спеціалізованих систем		екзамен
Всього по циклу:		32	
<u>ВБ3</u> <u>ДВС 2</u>	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	5,0	екзамен
<u>ВБ4</u> <u>ДВС 3</u>	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	5,0	екзамен
<u>ВБ5</u> <u>ДВС 4</u>	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	6,0	екзамен
<u>ВБ6</u> <u>ДВС 5</u>	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	5,0	екзамен
<u>ВБ7</u> <u>ДВС 6</u>	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	5,0	екзамен
<u>ВБ8</u> <u>ДВС 7</u>	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	5,0	екзамен
Всього по циклу:		31	
Загальний обсяг вибірових компонент:		63	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

(Із змінами, внесеними відповідно до рішення вченої Ради ДонНТУ від 27.02.2025 р., протокол №2, введено в дію наказом від 27.02.2025 р. № 61)

2.2. Структурно-логічна схема ОП



Структура освітньої програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. Рік вступу 2024 р.

1семестр		2семестр		3семестр		4семестр		5семестр		6семестр		7семестр		8семестр	
Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К
Іноземна мова. Частина 1	4	Іноземна мова. Частина 2	4	Філософія	4	Чисельні методи ІНД	6	Безпека та захист операційних систем	6	Криптографічні протоколи КП	6	Правознавство	5	Управління інформаційною безпекою	6
Вища математика. Частина 1 ІНД	7	Вища математика. Частина 2 ІНД	7	Теорія ймовірності та математична статистика	6	Організація баз даних КП	5	Теорія сигналів та процесів ІНД	6	Інформаційно-телекомунікаційні системи ІНД	5	Безпека життєдіяльності ІНД	4	Методи та засоби технічного захисту інформації	6
												Безпека програм та даних ІНД	5	Моніторинг безпеки функціонування ІКС та комп'ютерних мереж	6
Ділова українська мова	4	Історія України та української культури	5	Основи інформаційної безпеки КР	5	Системне програмування	5	Математичні методи криптографії ІНД	6	Архітектура систем захисту інформації (КСЗІ)	5	Захист розподілених баз даних та інформаційних систем	6	Технології створення криптографічних додатків	6
Фізичне виховання. Частина 1	3 залік	Фізичне виховання. Частина 2	3 залік	Об'єктно-орієнтоване програмування ІНД	5	Основи безпеки в Інтернет	5	Захист комп'ютерних мереж	6	Методи приховування інформації	5	Кібербезпека критичної інфраструктури, ІНД	5	Інформаційна безпеки спеціалізованих систем	
						Безпека Web-додатків		Протоколи передачі даних		Основи стеганографічних перетворень		Захист критичної інфраструктури, ІНД			
Фізика	7	Програмування ІНД	6	Комбінаторні методи захисту інформації ІНД	5 дз	ДВС3	5	ДВС4	6	ДВС5	5	ДВС6	5	ДВС7	5
Основи алгоритмізації ІНД	5	Дискретна математика	5	Додаткові розділи комбінаторного аналізу ІНД											
						ДВС2	5 дз	Навчальна практика	4			Виробнича практика	4		
	30		30		30		30		30		30		30		30

Освітні компоненти	
	Обов'язкові дисципліни загальної підготовки
	Обов'язкові дисципліни професійної підготовки
	Практики
	Атестації
	Дисципліни вільного вибору студента

3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників освітньої програми проводиться у формі Єдиного державного кваліфікаційного іспиту та завершується видачою документів встановленого зразка про присудження йому ступеня «Бакалавр з кібербезпеки та захисту інформації» зі спеціальності 125 Кібербезпека та захист інформації.

(Із змінами, внесеними відповідно до рішення вченої Ради ДонНТУ від 27.02.2025 р., протокол №2, введено в дію наказом від 27.02.2025 р. № 61)

4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Позначки програмних компетент- ностей та освітніх компонентів	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК01	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК02	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК03			+					+					+																				+	+	+	
ЗК04	+				+																												+	+	+	
ЗК05	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК06			+									+																					+	+	+	
ЗК07			+									+																					+	+	+	
ЗК08	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ФК01	+					+						+	+				+					+	+			+		+		+	+	+	+	+	+	
ФК02											+		+			+	+		+					+	+	+		+		+		+	+	+	+	
ФК03															+		+			+						+				+			+	+	+	
ФК04																	+					+		+	+	+		+	+	+	+	+	+	+	+	
ФК05																	+				+	+	+			+		+		+		+	+	+	+	
ФК06													+	+			+	+			+		+	+	+	+	+	+			+	+		+	+	
ФК07																	+											+			+			+	+	+
ФК08		+			+		+							+		+	+	+	+		+		+	+	+			+					+	+	+	
ФК09		+			+		+							+							+		+								+		+	+	+	
ФК10		+			+		+				+						+	+	+			+				+		+	+	+	+	+	+	+	+	

Примітки:

- ОКі - певний обов'язковий компонент освітньої програми за розділом 2.1;
- ВБі - певний вибірковий блок освітньої програми за розділом 2.1;
- ЗКі - загальна компетентність за розділом 1.6 профілю освітньої програми;
- ФКі - спеціальна (фахова) компетентність за розділом 1.6 профілю освітньої програми;
- - позначка, яка означає, що певна програмна компетентність забезпечується певним освітнім компонентом поточного рядка.


5. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ (ПРН) ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

Позначки програмних результатів освітніх компонент	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	
ПРН01	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН02	+					+					+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ПРН03	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН 04	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН 05	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН 06	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН07		+			+		+				+					+	+			+		+	+	+	+	+					+	+		+	+	
ПРН 08		+			+		+				+					+	+		+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН 09												+					+			+					+	+	+	+	+	+	+	+	+	+	+	+
ПРН 10														+	+	+	+	+			+				+	+	+	+	+	+	+	+	+	+	+	+
ПРН 11																	+					+					+			+	+	+	+	+	+	+
ПРН 12																+	+					+					+	+	+	+	+	+	+	+	+	+
ПРН 13																	+				+	+					+			+	+	+	+	+	+	+
ПРН 14																				+		+					+		+	+	+	+	+	+	+	+
ПРН 15	+														+		+			+		+						+		+	+	+	+	+	+	+
ПРН 16																	+										+			+	+	+	+	+	+	+
ПРН17																						+		+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН18																+									+	+					+	+	+	+	+	+
ПРН19																						+									+	+	+	+	+	+
ПРН20																		+				+					+	+		+	+	+	+	+	+	+
ПРН21																	+						+				+	+		+	+	+	+	+	+	+

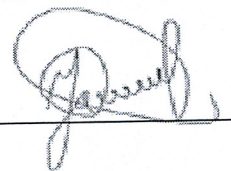
Примітки:

1. РНі - певний результат навчання за розділом 1.7 профілю освітньої програми;
2. • - позначка, яка означає, що певний програмний результат забезпечується освітнім компонентом поточного рядка.

Зав. кафедри прикладної математики та інформатики



Наталія МАСЛОВА



Ярослав ДОРОГИЙ

Гарант освітньої програми